REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
28-03-2012	Master of Military Studies Research Paper	September 2011 - April 2012

4. TITLE AND SUBTITLE
Offensive Cyber is Fires, A Case for MAGTF Integration

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Torres, Angel M.
Maj, USMC
CSC AY12

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
N/A

12. DISTRIBUTION AVAILABILITY STATEMENT
Unlimited

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT
The introduction of offensive cyber operations into the Marine Air Ground Task Force (MAGTF) requires a member of the staff include cyber operations in their capability integration. Cyber operations are at the forefront of our national strategic discussion. The Marine Corps has taken on a very proactive approach to this vaguely defined but ever vital domain. This paper argues that the integration of offensive cyber operations into MAGTF operations need to be integrated by the already established fire support coordinator billet. This paper initially looks takes a historical overview and presents perspectives of the current strategic environment. Historic U.S. action has been defensive. Other state and non-state actors have already executed offensive operations. As the Marine Corps continues to validate and train to their current strategy including the cyber domain, a staff member of the MAGTF needs to take on the role of not just establishing or defending networks, but also integrating offensive cyber operations into MAGTF operations. The Fire Support Coordinator is best suited to conduct the integration of offensive cyber operations into a combined arms operation.

15. SUBJECT TERMS
Fires, Artillery, Cyber, MAGTF Integration, FSC, Fire Support Coordinator, Offensive Cyber Operations

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Marine Corps University / Command and Staff College
Unclass	Unclass	Unclass	UU	31	19b. TELEPONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE:
Offensive Cyber is Fires, A Case for MAGTF Integration

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR:
Major Angel M. Torres, III, USMC

AY 11-12

Mentor and Oral Defense Committee Member: Edward Erickson, PhD
Approved: Edward Erickson
Date: 28 March 2012
Oral Defense Committee Member: Pauletta Otis, PhD
Approved: Pauletta Otis
Date: 28 March 2012

Executive Summary

Title: Offensive Cyber is Fires, A Case for MAGTF Integration

Author: Major Angel M. Torres, III, United States Marine Corps

Thesis: The introduction of offensive cyber operations into the Marine Air Ground Task Force (MAGTF) requires a member of the staff include cyber operations in their capability integration.

Discussion: Cyber operations are at the forefront of our national strategic discussion. The Marine Corps has taken on a very proactive approach to this vaguely defined but ever vital domain. This paper argues that the integration of offensive cyber operations into MAGTF operations need to be integrated by the already established fire support coordinator billet. This paper initially looks takes a historical overview and presents perspectives of the current strategic environment. The historic U.S. action has been defensive. Other state and non-state actors have already executed offensive operations. As the Marine Corps continues to validate and train to their current strategy including the cyber domain, a staff member of the MAGTF needs to take on the role of not just establishing or defending networks, but also integrating offensive cyber operations into MAGTF operations.

Conclusion: The Fire Support Coordinator is best suited to conduct the integration of offensive cyber operations into a combined arms operation.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Table of Contents

Acknowledgments

This paper is dedicated to my wife, Natalie. Her patience and assistance allows me to persevere.

Introduction

"Every Marine a Rifleman" goes the popular ethos that embodies the Marine Corps legacy since 1775. This phrase, practical and applicable in yesterday's battlefields, will remain applicable in the future. Lieutenant General Lewis B. "Chesty" Puller once enhanced this ethos by proclaiming, "Old breed? New breed? There's not a damn bit of difference so long as it's the Marine breed"[1]. The world has changed quite a bit from those times to the present world where the Department of Defense (DoD) and the Marine Corps have moved forward with the naming of a new domain regarding the future of warfare: cyberspace. Cyber operations have greatly affected the use of networks and technology in the modern battlefield. The systems allowing these assets to command and control, communicate, and target in the modern battlefield have evolved and continue to do so as we move forward in military affairs. Which primary or special staff member within the Marine Air Ground Task Force (MAGTF) is best suited to integrate cyber warfare into a combined arms operation? This question requires an in-depth answer, one that may exist in our current structure and doctrine. The MAGTF needs to establish the coordinator and integrator of these operations in this domain. The MAGTF is beginning to embrace cyber operations and has initially taken a defense-in-depth approach to dealing with this threat. Marine Cyber Command establishes cyber warriors, those best suited to begin the technical fighting in this domain. The application of offensive cyber operations into the Marine Air Ground Task Force (MAGTF) requires fire support coordinators to include cyber operations in their capability integration.

This paper addresses this issue by first establishing a historical starting point. Next, a review the current strategic environment is discussed. The current strategic environment and the

[1] Marine Corps Association, "Marine Corps Quotes," http://www.mca-marines.org/leatherneck/marine-corps-quotes (accessed Jan 29, 2012).

historic uses of cyber operations provides an overview of the current imminent issues regarding cyber operations and just how relatively new this domain is to the DoD rhetoric and to the Marine Corps. The next section addresses how contemporary cyber operations are being initially planned for with a defensive mindset and how potential adversaries are currently establishing a precedent in cyber network operations. The follow-on section discusses the Marine Corps' current strategy for cyber operations, focused at the strategic level. This section will lead into a discussion of the need for a planner within the MAGTF staff to embrace this domain's operational planning and integration into the combined arms fight. In conclusion, I establish how this coordination is transparently applied to an already conventional process that applies to cyber operation's capabilities and limitations.

Historical Starting Point of Cyberspace

What is cyber? Is this simply a fancy term for the Internet? A quick history follows explaining some key factors of the genesis of this domain that has come to affect every facet of American life. Leonard Kleinrock began toying with electronics at a very young age. Eventually, in 1961 he published a paper titled, "Information Flow in Large Communication Nets", that first introduced the concept of breaking digital messages into "packets".[2] In 1964 a Massachusetts Institute of Technology (MIT) book titled "Communication Nets" was published by Kleinrock. Here, basic principles of packet switching were introduced, thus providing the fundamental underpinnings which continue to provide a basis for today's Internet technology.[3] Eventually, through government funding, Kleinrock played a key role in preparing a functional specification for the Advanced Research Projects Agency Network (ARPANET) – "a

[2] University of California, "Personal History/Biography: the Birth of the Internet," http://www.lk.cs.ucla.edu/personal_history.html (accessed Jan 9, 2012).
[3] Ibid.

government-supported data network that would use the technology which soon came to be known as packet switching".[4] Through this government funded research, the Internet was born and as thus validated the claim that, "The Department of Defense invented the Internet, and the possibility of using it in warfare was not overlooked even in its early days."[5] The initial network used by the military was seen as a way to communicate with and command and control units throughout the world. At the time of its inception, the Soviet threat presented the biggest concern. Eventually, the Internet developed into an open network of networks. "From any network on the Internet, you should be able to communicate with any computer connected to any of the Internet's networks. Cyberspace includes the Internet *plus* lots of other networks of computers that are not supposed to be accessible from the Internet."[6] The other networks that are not supposed to be accessible from the public internet are what first make it vulnerable. Since the Internet boom in the 1990s, our nation has come to rely on this resource, so much so that our "…reliance on information technology and shared commercial networks in the battlefield raises concerns about attacks on the Nation's military forces and civilian infrastructures."[7] The Internet, cyberspace, and its functionality moved to the forefront of our nation's concerns as we entered the twenty-first century.

Review of the Current Strategic Environment

The Presidential and DoD guidance of January 2012 reemphasized the significance of cyberspace that the 2010 Quadrennial Defense Review (QDR) established. The QDR is the

[4] Ibid.
[5] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About it* (New York: Harper Collins Books, 2010), 34.
[6] Ibid, 70.
[7] Jacques S. Gansler and Hans Binnendijk, *Information Assurance: Trends in Vulnerabilities, Threats, and Technologies* (Washington, D.C.: National Defense University, 2004), 5-6.

Secretary of Defense's guidance for shaping the future of the U.S. military and is nested with the President's National Security Strategy. The January 2012 DoD guidance titled, *Sustaining U.S. Global Leadership: Priorities for the 21st Century Defense*, further echoed the President's guidance to, "…ensure that our military is agile, flexible, and ready for the full range of contingencies…we will continue to invest in the capabilities critical to future success…and prevailing in all domains, including cyber."[8] The 2010 Quadrennial Defense Review specifically directed the DoD to begin focusing on this new domain. "There is no exaggerating our dependence on DoD's information networks for command and control of our forces, the intelligence and logistics on which they depend, and the weapons technologies we develop and field."[9] This dependence manifested itself into a focus for the DoD and the naming of the new domain to go with our already established domains. "Although it is a man-made domain, cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space."[10] This domain has produced several situations where its integration has already occurred with the attack of one belligerent force against another. As the refined DoD guidance from January of 2012 emphasized, both state and non-state actors possess, "…the capability and intent to conduct cyber espionage and, potentially, cyber attacks on the United States, with possible severe effects on both our military operations and our homeland."[11]

As we will see in the proceeding section, the U.S. has established policy regarding offensive action in cyber operations. Within the Department of the Navy, specifically the Commandant of the Marine Corps shall: "Develop organizational constructs necessary to ensure

[8] Department of Defense, *Sustaining U.S. Global Leadership: Priorities for the 21st Century Defense*, http://www.defense.gov/news/Defense_Strategic_Guidance.pdf (accessed Jan 29 2012).
[9] Department of Defense, *Quadrennial Defense Review*, http://www.defense.gov/qdr/qdr%20as%20of%2029jan10%201600.PDF (accessed Jan 9 2012).
[10] Ibid.
[11] DoD, *Sustaining U.S. Global Leadership: Priorities for the 21st Century Defense*.

the exchange of information, tactics, techniques, and procedures between...Computer Network Defense (CND), Computer Network Exploitation (CNE), and Computer Network Attack (CNA) activities, units and personnel to optimize synchronization between these related fields and people."[12] Other countries have already begun their attacks.

Historical Examples of U.S. Cyber Operations and our Defensive Outlook

Dating back to the early 1990s, when the Internet was still in its nascent stage, there was an emphasis on military's bond with cyber operations. The large kinetic fight that begins this discussion is that of the Gulf War, Operation *Desert Storm*. The first cyber warriors began to plan with special operations commandos to neutralize the Iraqi air defense radars and missile networks. This attack would have occurred prior to the U.S.'s air and ground attacks, neutralizing the enemy effects on the coalition effort. Norman Schwarzkopf stated, "…'these snake-eaters had some crazy idea' to sneak into Iraq before the first shots were fired and seize control of a radar base in the south of the country…hook up to the Iraqi network from inside the base and then send out a program that would have caused all computers on the network all over the country to crash and be unable to reboot."[13] However, this plan did not proceed further than the planning stage and never materialized. The U.S. executed a kinetic attack of the targeted air defense and missile systems with air to ground and ground to ground assets in order to achieve its desired effects. This was a premature notion by those cyber warriors, but a step in the right direction.

[12] Secretary of the Navy, *Cyberspace Policy and Administration Within the Department of the Navy,* SECNAV Instruction 3052.2, (March 6, 2009), 5.
[13] Clarke, 9.

The technology boom of the 1990s enhanced our reliance on the cyber world. The world also changed after the attacks on the U.S. on September 11, 2001. The DoD and U.S.'s reliance on the internet and cyber networks escalated. In Afghanistan, during the first operation of the Global War on Terror, the percentage of precision weapons used increased to 60 percent of the total weapons used, and during *Iraqi Freedom*, the percentage was approximately 75 percent.[14]

Just thirteen years after our first hint of cyber attack operations by the U.S., estimates indicate that the forces in Iraq for Operation *Iraqi Freedom* required ten times the communication bandwidth used during Operation *Desert Storm*.[15] The cyber operations conceived for this operation are not solely used for protecting the global positioning system (GPS) guided munitions, or command and control bandwidth. These uses fall into the defensive side of cyber operations. Regarding offensive cyber operations, there was also a plan that the U.S. primarily conceived, similar to that of the Gulf War. Specifically, thousands of Iraqi military officers received e-mails on the Iraqi Defense Ministry e-mail system just before the war started.[16] E-mails, to be used as psychological operations against these leaders, were meant to convince them that it was not worth the risk of fighting the U.S. during the initial invasion. This was the extent of offensive cyber operations during this phase of the war. The thought of neutralizing the enemy air defense networks was also vetted but not executed.

One use of cyber war is to make a conventional attack easier by disabling the enemy's defenses. Another use of cyber war is to send propaganda out to demoralize the enemy, distributing e-mails and other Internet media in place of the former practice of dropping

[14] Gansler, 16.
[15] Ibid, 16.
[16] Clarke, 9.

pamphlets.[17] The hesitation with the network attack was due to the "…Bush Administration…apparently unwilling to destroy Saddam Hussein's financial assets by cracking into the networks of banks in Iraq and other countries. The capability to do so existed, but government lawyers feared that raiding bank accounts would be seen by other nations as a violation of international law, and viewed as a precedent.[18] The precedent that was feared to be established was clearly not going to be set by the U.S. with the last major conflict of the twentieth century, nor with the first major conflict of the twenty-first century. Ideally our allies and potential enemies of the twenty-first century would feel the same way. Obviously, this is too optimistic a view.

Worldwide Application by State and Non-State Actors

In 2007, Israel began to deal with intelligence collected regarding Syria and a partially finished nuclear reactor built with North Korea's help. Israel devised a plan that would use an air to surface attack to neutralize this threat. Israel knew that they would require entering hostile air space that was clearly being monitored by Syrian air defense systems. The vulnerability, as Israel exposed, was the network that this system operated on. Throughout the attack, Syrian forces on the ground were confused and bewildered by the lack of pings on their radar system from the enemy that was attacking them from above. "What Syrians slowly, reluctantly, and painfully concluded the next morning was that Israel had 'owned' Damascus's pricey air defense network the night before. What appeared on the radar screens was what the Israeli Air Force had put there, an image of nothing."[19]

[17] Ibid, 11.
[18] Ibid, 10.
[19] Ibid, 4.

Clearly, the cyber attack was successful and Israel was able to accomplish its mission. This confusion is what was first envisioned by the U.S. for the Gulf War and later on for Operation *Iraqi Freedom*, but never executed. Syria was surprised. Computer hackers and cyber warriors, on the other hand, were not. Cyber War was clearly moving forward and materializing as a very effective weapon system. Once the cyber fires were integrated into their fire support plan, the Israeli concept of their military operations was able to effectively use their cyber superiority to have the kinetic effects on the ground that they desired. Cyber Wars in this context specifically refers to, "…actions by a nation-state to penetrate another nation's computer or networks for the purposes of causing damage or disruption."[20] As an ally of the U.S., Israel began to set the precedent with offensive cyber operations.

That same year, the offensive nature of cyber operations was also conducted by the Russians without the integration of a military attack. This is the now famous Estonia case study for cyber operations. Estonia, a former Soviet-era territory, is one of the most technologically wired nations in the world. Estonian's use of the Internet in everyday life is well ahead of that of the American's. Estonia is "…rank(s), along with South Korea, well ahead of the United States in the extent of its broadband penetration and its utilization of Internet applications in everyday life."[21] What Russia was accused of doing was attacking Estonian networks with a distributed denial-of-service (DDOS) attack. [22] This attack takes over a computer network and sends messages back to its parent network. The more of these messages that get sent back, the more digitally clogged the system gets, eventually shutting down the network. This attack was not synchronized with a kinetic element's maneuver, but nonetheless, Estonia was shut down from

[20] Ibid, 6.
[21] Ibid, 13.
[22] Ibid, 13.

the outside world during this attack. Cyber security experts "followed the attacking pings to specific zombie computers and then watched to see when the infected machines "phoned home" to their masters…Estonia claimed that the ultimate controlling machines were in Russia, and that the computer code involved had been written on Cyrillic-alphabet keyboards."[23] This attack was the first of Russia's publicized engagements in the international community with cyber operations. They soon saw the potential for this capability when integrated with a kinetic force that Israel also demonstrated in 2007.

In 2008, the Russians were able to carry out the integration of a cyber attack with a ground maneuver force. This occurred when it invaded the former Soviet Republic of Georgia. While the Russian army prepared to move into combat operations, their cyber warriors began their attack as well. "Their goal was to prevent Georgians from learning what was going on, so they streamed DDOS attacks on Georgian media outlets and government websites. Georgian's access to CNN and BBC websites were also blocked."[24] The Georgian's ability to conduct command and control of their forces, have seamless contact with the outside world, and to communicate their predicament was limited, giving the Russian army the advantage that they needed to execute their successful assault. The attacks were synchronized to achieve maximum effect against the Georgians. The cyber attacks, "…picked up in intensity and sophistication just as the ground fighting broke out…" against the Georgians' defenses. [25] The task and purpose of this integrated attack had the effect of having the Georgians effectively lose control of the nation's ".ge" domain and forcing Georgia to shift many government websites to servers outside

[23] Ibid, 15.
[24] Ibid, 18.
[25] Ibid, 19.

the country.[26] This kind of attack, another great example of offensive cyber operations, brought the Russians further into the cyber discussion.

Recent American Application

The U.S. has a reason to fear the effects of cyber attacks, especially if a likely enemy integrates it with more lethal follow-on effects and elements. The above examples outline possible scenarios and easily bring discomfort to the minds of cyber warriors and others that protect the U.S.'s interests. Even though we see this domain ahead in our defense policy, we have yet to openly carry out the integration of a cyber attack with a ground assault. Even during the recent Libyan bombing campaign that supported the protesters of Muammar el-Qaddafi's regime, the U.S. opted out of this course of action. President Barrack Obama debated this kind of warfare before deploying the U.S. forces in support of this operation. Once again, the U.S., "…fearing that it might set a precedent for other nations…[was] unable to resolve whether the president had the power to proceed with such an attack without informing Congress.[27] Such a new domain without fully understood or developed capabilities and practices seemed too big of a leap for the U.S. in Libya in early 2011. Regarding this conflict that ended successfully, even without a specific cyber attack, a President Obama administration official stated, "These cyber capabilities are still like the Ferrari that you keep in the garage and only take out for the big race and not just for a run around town"[28] Regardless, President Obama and Secretary of Defense Leon Panetta have been clear in establishing cyber network operations as key to our current and future security policies.

---

[26] Ibid, 19.
[27] Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Lybia," *New York Times*, October 17, 2011.
[28] Ibid.

Recruiting the new cyber warriors that will establish the protected networks and one day execute offensive cyber operations has been a challenge due to the complexity and technical skills required for this specialty. The U.S. Air Force has embraced this mandate from the President and the Secretary of Defense and the employment of cyber warriors. A recent Air Force commercial targets the cyber warrior by presenting them the significance of the networks that they will protect and the future that this domain still has. The commercial highlights that, "…control of power systems…water systems…that is the new battlefield…in the future this is going to be the premier warfighting domain…this is going to be where the major battles are fought…I am an Air Force Cyber Warrior."[29] When folks working on computer codes are visiting sites and networks that they are not authorized, hackers become cyber criminals. When they work for the U.S. military, we call them cyber warriors.[30] The Air Force is anticipating a domain where battles are going to be fought, a domain that already has a history of battles being fought by nation-states such as Russia. This transition from a defensive mindset to an offensive mindset has not been easy, but it is required in order to maintain relevance in the domain. As Lieutenant General Robert Elder, the former director of the Air Force Cyberspace Operations Task Force, states, "If you are defending in cyberspace, you're already too late. If you do not dominate in cyberspace, you cannot dominate in other domains. If you are a developed country [and you are attacked in cyberspace], your life comes to a screeching halt."[31] Estonia knows this too well.

Cyber attacks evidenced by other state and non-state actors was a catalyst for the USMC to focus on cyber operations. The tactical level Marine Air Ground Task Force unit commander

[29] Clarke, 33.
[30] Ibid, 72.
[31] Ibid, 36.

needs to conduct kinetic missions to preserve the freedom of action and strategic advantage in cyberspace which will allow for freedom of action in the other domains that the Marine Corps operates in. A clear concern for the U.S. as we continue to move further into the twenty-first century is the competitive development that nation-states like China will have on the U.S.'s influence in the Pacific and the rest of the world. As an expeditionary force in readiness, the Marine Corps cannot wait to act in offensive cyber operations when it first engages in an offensive cyber fight. "…China will not be the equal of the U.S. military for many decades. However, if China can use asymmetrical tactics like cyber war, it believes the new, modern Chinese forces would be sufficiently advanced to take on U.S. forces that will have been crippled by Chinese cyber attack."[32] When a forward deployed MAGTF is simply on the defensive side of a cyber war, cyber warfare then becomes a one-sided battle where the attacker makes all the strikes and the target of the attack responds so slowly that the attacker usually gets away without being identified.[33] Timely responses, integrated with the MAGTF commander's intent for cyber operations are required to prevent such a scenario where U.S. assets are losing the cyber fight and its effects are felt not only by the forward deployed military forces, but also in the U.S. by the affected civilian population. Although operating as a forward deployed force, if not ready for a cyber attack and possessing cyber superiority, cyber experts believe that, "No flotilla of ships or intercontinental missiles or standing armies can defend against such remote attacks located not only well beyond our borders but beyond physical space, in the digital ether of cyberspace."[34]

[32] Ibid, 54-55.
[33] Norman Howes, Michael Mezzino, and John Sarkesain, *On Cyber Warfare Command and Control Systems*, (Washington, D.C.: Missile Defense, 2004), 2.
[34] Ibid, 71.

Marine Corps' Current Strategy for Cyber Operations

The Marine Corps has reacted to the guidance that it has received regarding cyber space by establishing Marine Forces Cyber. As Lieutenant General George J. Flynn, the then-Deputy Commandant for Combat Development and Integration stated before Congress, "The Marine Corps has established the Marine Forces Cyber (MARFORCYBER) to focus its cyber efforts. In coordination with United States Cyber Command (USCYBERCOM), MARFORCYBER will plan, coordinate, integrate, synchronize and direct *defensive* cyberspace operations to *preserve* the Marine Corps ability to use and function within the Marine Corps Enterprise Network (MCEN)."[35]

Now that the Marine Corps has an established unit, it needs to man, train and equip these forces. For that, "…the Marine Corps will dedicate approximately 800 personnel to the "pure" cyber workforce."[36] The training that will come to these cyber Marines will come from the Joint Cyber Analysis Course (JCAC) and the Joint Network Attack Course (JNAC).[37] LtGen Flynn also specifies the initial intent for operational cyber capabilities by describing that, "MARFORCYBER and Marine Cryptologic Support Battalion (MCSB) Company L provide resources for National and Joint kinetic attack requirements; deployed forces in support of ongoing operations in Afghanistan; as well as, direct support to USCYBERCOM collaborative planning efforts."[38]

MCSB is a Marine Cryptologic Support Battalion. Its companies range the length of the alphabet until reaching Company L. The companies have missions ranging from cryptology to

[35] House of Representatives Subcommittee on Terrorism, Unconventional Threats and Capabilities of the House Armed Services Committee, *Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations,* September 23, 2010.
[36] Ibid.
[37] Ibid.
[38] Ibid.

signals intelligence. Company L, based out of Fort Meade, Virginia, and therefore co-located with USCYBERCOM is specifically set up to support the cyber domain from the USMC's perspective. Its mission is to, "plan and execute offensive cyberspace operations in order to support Joint and Service requirements."[39] The Company has a growing capacity to respond directly to tasks from Joint Task Force Commander.[40] This growing company sized element supports the planning and execution of offensive cyber operations for the Marine Corps as a whole, as stated in its mission statement. It has a coordinating relationship, not a direct support mission, thereby limiting the organically possessed MAGTF offensive cyber capabilities.[41] It can provide a duty expertise to the MAGTF that will use it through its reach-back coordinating relationship with USCYBERCOM. Company L is the Marine Corps' liaison to USCYBERCOM. Operationally, a staff officer within the MAGTF is still required to integrate the effects of the cyber domain into the overall plan.

A Planner Within the MAGTF

There are some clearly defined staff sections that will encompass the cyber responsibilities. First off are the Communications and Information Systems integrators, the G-6. Marine Corps Doctrinal Publication 5-12, Organization of Marine Corps Forces, tasks this section with the responsibility of the formulation of Communications and Information Systems (CIS) plans and policies for the MAGTF. Although doctrinally the MAGTF Command Element has the CIS resources to establish its internal requirements, the cyber jump and decentralized

[39] United States Marine Corps, *Company L*, http://www.marines.mil/unit/hqmc/intelligence/mcia/mcsb/Pages/CompanyL.aspx (accessed 12 February 2012).
[40] Headquarters U.S. Marine Corps, *USMC Cyberspace Concept* (Washington, DC: U.S. Marine Corps July 17, 2009), 13.
[41] Ibid, 18.

operations have forced this section to shift much of its focus.[42] The MAGTF Command Element's communications detachment is responsible for the installation, operation, and maintenance of pertinent MAGTF local area networks (LANs), wide area networks (WANs), and for its defense through Information Assurance.[43] This section and its leadership establish the network and allow for its use in order to maximize command and control up and down the chain of command. Some cyber warriors will be managed and employed by the leadership in this section. The duty-expertise on the system's capabilities and limitations will be maintained by this section.[44] The "data guys" in this section do not immediately employ the capability of integrating cyber operations, they execute cyber operations. This section facilitates planning by providing the Operations Section the capabilities and limitations of its command and control systems in the proposed course of action while conducting its day-to-day operations.

The Radio Battalion element of the MAGTF augments this section's capabilities and affects intelligence gathering. The Radio Battalion provides signals intelligence (SIGINT), ground-based electronic attack (EA), communications security (COMSEC) monitoring, and special intelligence (SI) communication support to the MAGTF.[45] This unit is another place where cyber warriors will be found in the MAGTF. These are some elements of cyber operations, but not all. The electronic warfare and air officers of the operations section also integrates other Electronic Attack capabilities. Clearly, there are plenty of hands in the cyber domain that if not fully integrated into the overall operation, have the potential of producing unsynchronized results and possibly opening up vulnerabilities for cyber attacks.

---

[42] Ibid, 18-19.
[43] Headquarters U.S. Marine Corps, *Organization of Marine Corps Forces*, MCRP 5-12 (Washington, DC: U.S. Marine Corps, October 13, 1998), 6-2.
[44] Hq USMC, *USMC Cyberspace Concept*, 23.
[45] Hq USMC, MCRP 5-12, 6-6.

The Norman Howes article titled, "On Cyber Warfare Command and Control Systems", raises an analogy of the type of hierarchical organization that the MAGTF has in the cyber domain. The MAGTF, "…relies on situation reports going up the chain of command for decision making and orders coming back down the chain of command that implement these decisions, [this] does not work well for cyber defense."[46] The separate sections involved can pose a delay in action and reaction for offensive cyber warfare. The MAGTF can face the reality of one day having cyber inferiority in a hostile environment. In tis article, Norman Howes also discusses the Marine Corps' concept of maintaining tempo over the enemy. This is highlighted in Marine Corps Doctrinal Publication 1, *Warfighting*, and applied to the cyber domain, as the importance of continuing to keep the enemy reacting to our actions in order to maintain momentum in cyber space. The article specifies the significance of this capability in the cyber domain. The MAGTF should not make a full pendulum swing and negatively react to this possible effect by flattening our established command and control structure. Specifically, the article states that,

> Cyber battles usually take place in the seconds to minutes range whereas kinetic warfare battles occur in the hours to days range. Consequently, we cannot hope to use the kinetic warfare organizational model of command and control effectively for cyber warfare. On the other hand, we do not want to lose the kinetic warfare command structure when we integrate cyber warfare C2 into the overall kinetic warfare command and control.[47]

The dilemma posed above demonstrates the differences in the cyber world. These differences can be mitigated through adaptation to the cyber world, but also through innovation of the current command and control structures and relationships. "Each strategy element of kinetic warfare has a parallel in cyber warfare."[48] Referencing Marine Corp Operations 1-0's definition

[46] Howes, 4.
[47] Ibid, 4.
[48] Ibid, 5.

of fires, ("The use of weapon systems to create a specific lethal or nonlethal effect on a target."[49]), offensive cyber operations' parallel in conventional operations are fires. The Marine Corps can adapt to the unique capabilities of offensive cyber operations by having an already established staff officer integrate these fires into the planning process.

Cyber as "Fires" in an Already Conventional Process

Accepting the fires-cyber parallel the Fire Support Coordinator is the new cyber space parallel from kinetic warfare to cyber warfare that needs to integrate all of these aspects into a combined arms operation for the MAGTF. Although a special staff member, the Fire Support Coordinator is represented at the table of operational planning teams alongside the maneuver, intelligence, logistics, etc. functions. He provides the integration of fires functions into MAGTF operations. Doctrinally, in a kinetic fight, and per the Marine Corps Warfighting Publication 3-16 (Fire Support Coordination in the Ground Combat Element), the Fire Support Coordinator (FSC) has very specific roles. The FSC, "…create[s] effects on enemy forces or functions that contribute to [the commander's] mission accomplishment."[50]

With fires, the FSC can shape the battlefield by, "…attacking the enemy's center of gravity (COG) through enemy critical vulnerabilities and creating decisive combat power with a combined arms effect."[51] In his work, *On War*, Carl Von Clausewitz clarifies this COG stating that, "…one must keep the dominant characteristics of both belligerents in mind. Out of these characteristics a center of gravity develops, the hub of all power and movement, on which

---

[49] Headquarters U.S. Marine Corps, *Marine Corps Operations*, MCDP 1-0 (Washington, DC: U.S. Marine Corps, August 9, 2011), Glossary 1-4.
[50] Headquarters U.S. Marine Corps, *Fire Support Coordination in the Ground Combat Element*, MCWP 3-16 (Washington, DC: U.S. Marine Corps, November 28, 2001), 1-2.
[51] Ibid, 1-2.

everything depends."[52] COG examples such as the military forces, nation capitals, the will of the people, logistical lines of communication, and command and control systems, can all be affected by the critical vulnerabilities that are accessible through cyber attacks and cyber terrorism. The Israeli and Russian examples point out that the only distinction between computer network exploitation and attack is the intent of the cyber terrorist or cyber warrior in front of the computer. Essentially, "The skill sets needed to penetrate a network for intelligence gathering purposes in peacetime are the same skills necessary to penetrate that network for offensive action during wartime."[53] This vulnerability through synchronized cyber attacks can have poor results for the affected force. Against these types of threats, cyber attacks need to be integrated seamlessly in a combined arms fight, that may only have a virtual battlefield.

Marine Corps doctrine continues to direct our attention to the Fire Support Coordinator when we begin to have offensive cyber campaigns integrated with the combined arms capabilities of the Marine Corps. As fires, offensive cyber operations are capable of creating very specific effects on targets, as seen in the Israel-Syrian example of attacks on air defense systems. Our current doctrine continues to be valid when we see the integration of this new domain into our concepts of operations. Although attacking potential enemies through DDOS or network denial, the FSC's role remains constant. Now, he must be able to receive intelligence that is being gathered through cyber means by cyber warriors in the intelligence community in order to enter the same targeting process that is currently established in the Marine Corps Planning Process. The integration of this new type of fire support into the scheme of maneuver continues to require the same, "…precise arrangement of coordinated activities in time, space,

---

[52] Carl von Clausewitz, *On War*; ed. Michael Howard and Peter Paret, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1984) 595.
[53] Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, (McLean, VA: Northrup Grumman, October 9, 2009), 8.

and purpose to produce the most effective fires" as it does in a conventional fight.[54] The FSC is still required to provide "…the right attack means delivered on the right target at the right time, creating a combined arms effect."[55] The new cyber domain will require more coordination with higher and adjacent cyber warriors as the fire support plan for cyber operations is carried out. Continuing to rely on an already established structure from the conventional special staff member of Fire Support Coordinator allows for continued integration throughout an operation as well as promoting the Marine Corps' single-battle concept. This concept is in even more harmony with the cyber domain, as our previously discussed dependence on the cyber realm has made our connectivity to more echelons a virtual reality. The single-battle concept promotes a "…unifying perspective of operations, which holds that actions anywhere in the operational environment can affect actions elsewhere."[56] The FSC as the cyber operations integrator presents itself as doctrinally consistent for the future battlefield within the cyber domain.

Recommendation

Many of the capabilities of the cyber domain are yet to be fully understood or achieved. Regardless, the responsibility that our civilian and military leadership has charged the Marine Corps with in this domain cannot be marginalized. Effectively, we are subject to Metcalfe's Law regarding our use and dependence of networks. This law states that "…although the cost of adding nodes to a network increases linearly, the utility of a network increases proportionately with the square of the number of users…as the number of military users added to the network

[54] Hq USMC, MCWP 3-16, 1-2.
[55] Ibid, 1-2.
[56] Hq USMC, MCDP 1-0, 3-2

increases, the value of the network would increase dramatically."[57] The military networks and nodes are closely tied to our command and control capabilities. This is currently a valid threat and it will continue to be so in the future. Beginning to have our FSCs learn the cyber domain limitations and capabilities today will allow the Marine Corps to head in the correct direction before we become reactive in this domain and lose our tempo against our enemy. This does not mean that every Fire Support Coordinator needs to be a cyber warrior in front of a computer screen. The Fire Support Coordinator needs to know the capabilities and limitations of the fire support systems that he integrates into the combined arms fight. The Fire Support Coordinator does not necessarily need to know how to fly the attack helicopter or how to be a mortar section chief in order to know how to integrate those weapon system's lethal applications into a combined arms fight. The parallel to the cyber domain requires the Fire Support Coordinator's understanding of the capabilities and limitations of the cyber domain and know that, as Russia and other countries have successfully concluded, offensive cyber operations are capable of being integrated alongside a maneuver plan. The Fire Support Coordinator within the MAGTF does not need control the direct employment of the cyber weapon systems, but to clear the fires that they produce per the concept of fires that is established.

Similar to the above analogy, the Fire Support Coordinator does not command the attack squadron or the mortar platoon that he integrates into the combined arms fight. The fire support coordinator knows how to leverage their capabilities into the combined arms fight. Specifically, in the cyber domain, the Fire Support Coordinator may never even know the cyber warrior that he is integrating into the maneuver plan. "It is possible for a *cyber warrior* to be in multiple virtual cells simultaneously…Cyber warfare commanders can be members of multiple lower

[57] Gansler, 17.

level virtual cells, multiple *peer cells* (virtual cells at their own level of command at other locations) and, if permitted, they can be members of higher-level virtual cells."[58] This reality is a shift from conventional fire support, but it does not need to be, and it is already aligned with the MCSB Company L capabilities and support relationship to a MAGTF. Similar to calls for fire (artillery and mortar fire support requests), and Joint Tactical Air Requests (JTAR), the cyber domain has developed, through Cyber Command, a request parallel in the cyber domain: a cyber effects request form. This form serves as the initiator for cyber effects similar to the call for fire or the JTAR. The targeting cycle can continue to be applied to the cyber domain as center of gravity and critical vulnerabilities are identified in order to fill fire support tasks that will integrate those desired effects into the maneuver plan. When offensive cyber operations are integrated by the fire support coordinator, a seamless transition of doctrine occurs towards the cyber domain when we treat this new domain as another fire support element.

Antithesis

Establishing more duties to an already labored Fire Support Coordinator is a sensitive subject to many elements of the Marine Corps, especially dealing with cyber operations. The current structure has the cyber domain and cyber warrior functions leaning towards the communications and system integrators (CIS). The CIS element of the MAGTF is already tasked with providing the network and its defense per established doctrine. They provide the capabilities of the cyber warriors to the MAGTF, so they seem to be a likely candidate for the role of offensive cyber operations integrations. Similarly, the intelligence sections and their future habitual relationship with cyber warriors, seems like an adequate fit for the role of

[58] Howes, 4.

offensive cyber operations integration. What these two functions do not immediately possess is the seamless transition from the kinetic realm to the cyber realm of integrating fires into a combined arms fight. The MAGTF fire support coordinators do have this capabilities as discussed above.

Within the field artillery community, where MAGTF fire support coordinators originate, an understandable hesitation is expected due to the perceived notion of an already over-taxed community. At the end of Operation *Iraqi Freedom,* artillerymen stood proud after massing the 11th Marine Regiment on Baghdad and proving that the decade of combined arms exercises proceeding the first Gulf War showed the devastating power of the *King of Battle*. From this zenith, the artillerymen began to provide personnel for a decade's worth of *in lieu of* missions supporting the follow-on counterinsurgencies in Iraq and Afghanistan. Those opposed to a task organizational adaptation regarding *in lieu of* missions criticized that the artillery regiments became the, "…well of souls that provided personnel and units, up to battalion strength, for any and all nonstandard missions that were required."[59] Based on this reassignment, and a possible future of integration of offensive cyber operations, many artillerymen would continue to feel that a generation of officers and cannon crew-men will not be able to function within their primary specialty of providing first-round fire for effect in combined arms operations. The integration of the fires domain is not going to bring cannon crewmen from the gun-line to become cyber warriors. The stated concern by artillerymen, that, "As a result of the structuring of the force after Operation IRAQI FREEDOM I (OIF I), the artillery community fell from the preeminence it enjoyed as the premier all-weather fires capability of the Marine Corps to the role of force provider for nearly everything except fire support…" is warranted, but not completely applicable

[59] Michael D. Grice, "Resuscitating the King," *Marine Corps Gazette*, October 2008, 21.

to the task of offensive cyber operations to fire support coordinators.[60] Offensive cyber integrations are a parallel application of fires in the cyber domain, not a distinct *in lieu of* mission.

Artillery officers need to continue to develop and maintain an image of a dependable weapon of choice for senior MAGTF commanders. With the cyber world affecting fire support coordination cells, the artillerymen affected are those officers serving as Fire Support Coordinators working alongside maneuver elements at their respective echelon. This does not mean that the Regiments (and their higher headquarters) develop non-doctrinal "effects" cells that lump everything from key leader engagement to handbill generation and distribution to kinetic fires.[61] The cyber warriors (065X specialty) would augment the capabilities of breaking the enemy's will to fight using offensive cyber methods, while being integrated as fires.

Conclusion

The Fire Support Coordinators need to know the capabilities and limitations of the cyber domain. With that knowledge, they need to integrate those capabilities and limitations into the combined arms fight. The cyber warriors that come to the targeting boards hosted by the Fire Support Coordinator need to come ready to engage in a fires discussion. This will not be an easy task, as embracing new capabilities rarely is. The top-down approach that the U.S. is currently pursuing with the cyber domain is warranted and a step in the right direction. A Fire Support Coordinator will not simply sit down with a Lance Corporal capable of hacking computer networks. He will expand his targeting board to encompass cyber warriors, and the legal advisor

[60] Ibid, 20-21.
[61] Ibid, 22.

to the commander and fully embrace the intelligence section's cyber analysis. A MAGTF Fire Support Coordinator will not be doing this alone. Due to the vast area of influence that the cyber hacker can affect, the Fire Support Coordinator and the cyber warriors will need to integrate their offensive cyber attacks at many levels. A feasible reality in the cyber world is one where a secret internet protocol address and connection can allow for lower echelons to contact, coordinate, and view the virtual worlds all the way through Marine Forces Cyber and Cyber Command, in real-time.

As we have entered the cyber domain with the DoD, and begin to establish its role within the Marine Corps, we need to fully embrace this future of our force. The reality is that this is the next version of a Cold War. Instead of facing a possible Soviet nuclear attack, the U.S. faces the ability of a cyber hacker that can affect our civilian and military infrastructure simultaneously, without leaving his computer screen. In times of the next war, "…nation state attackers will launch multiple coordinated attacks against multiple targets using a variety of attack types. Such attacks will attempt to neutralize multiple layers of defense-in-depth assets simultaneously, leaving the systems on a network open to a second wave of attacks that create extensive damage that takes hours or days to repair."[62] This scenario is not only probable, it is possible. In order for our Marine Corps to continue to be the expeditionary force in readiness and maintain its image, it needs to maintain an edge in this new domain. By assimilating the capabilities of offensive cyber operations into our fire support coordination centers, the Marine Corps ensures the readiness and validity of its fire support integration into a combined arms fight capable of facing any modern battlefield—conventional or virtual. Not every Marine will be a cyber warrior, but the Fire Support Coordinator needs to know how to win with these cyber warriors.

[62] Howes, 5.

Bibliography

Borchgrave, Arnaud de, *Cyber Threats and Information Security: Meeting the 21st Century Challenge*. Washington, D.C.: Center for Strategic and International Studies, 2001.

Clausewitz, Carl von. *On War*; Edited by Michael Howard and Peter Paret. Translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1984.

Clarke, Richard A., and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About it*. New York: Harper Collins Books, 2010.

Department of Defense. *Defense Budget Priorities and Choices*. January 2012. http://www.defense.gov/news/Defense_Budget_Priorities.pdf (accessed 29 Jan 2012).

Department of Defense. *Quadrennial Defense Review*. February 2010. http://www.defense.gov/qdr/qdr%20as%20of%2029jan10%201600.PDF (accessed 9 Jan 2012).

Department of Defense. *Sustaining U.S. Global Leadership: Priorities for the 21st Century Defense*. January 2012. http://www.defense.gov/news/Defense_Strategic_Guidance.pdf (accessed January 29 2012).

Gansler, Jacques S., and Hans Binnendijk, *Information Assurance: Trends in Vulnerabilities, Threats, and Technologies*. Washington, D.C.: National Defense University, 2004.

Grice, Michael D. Grice. "Resuscitating the King." *Marine Corps Gazette*, October 2008.

Headquarters U.S. Marine Corps. *Warfighting*. MCDP-1. Washington, DC: Headquarters U.S. Marine Corps, June 20, 1997.

Headquarters U.S. Marine Corps. *Marine Corps Operations*. MCDP 1-0. Washington, DC: Headquarters U.S. Marine Corps, August 9, 2011

Headquarters U.S. Marine Corps. *Organization of Marine Corps Forces*. MCRP 5-12. Washington, DC: Headquarters U.S. Marine Corps, October 13, 1998.

Headquarters U.S. Marine Corps. *Fire Support Coordination in the Ground Combat Element*. MCWP 3-16. Washington, DC: Headquarters U.S. Marine Corps, November 28, 2001.

Headquarters U.S. Marine Corps. *USMC Cyberspace Concept.* Washington, DC: U.S. Marine Corps July 17, 2009.

Howes, Norman, Michael Mezzino, and John Sarkesain. "On Cyber Warfare Command and Control Systems." Washington, D.C.: Missile Defense, 2004.

Janczewski, Lech J., and Andrew M. Colarik, *Cyber Warfare and Cyber Terrorism*. Hershey, PA: IGI Global, 2008.

Krekel, Bryan. "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation." McLean, VA: Northrup Grumman, October 9, 2009.

Marine Corps Association. "Marine Corps Quotes." http://www.mca-marines.org/leatherneck/marine-corps-quotes (accessed January 29, 2012).

Potter, Evan H., *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*. London: McGill-Queens University Press, 2002.

Schmitt, Eric and Thom Shanker. "U.S. Debated Cyberwarfare in Attack Plan on Lybia." *New York Times*, October 17, 2011.

Secretary of the Navy. *Cyberspace Policy and Administration Within the Department of the Navy*. SECNAV Instruction 3052.2. Washington, DC : Department of the Navy, March 6, 2009.

Sengupta, Somini. "Phone Hacking Tied to Terrorists." *New York Times*, November 26, 2011.

U.S. Congress. House of Representatives. Subcommittee on Terrorism, Unconventional Threats and Capabilities of the House Armed Services Committee. *Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations*. September 23, 2010.

United States Marine Corps. "Company L." http://www.marines.mil/unit/hqmc/intelligence/mcia/mcsb/Pages/CompanyL.aspx (accessed 12 February 2012).

University of California. "Personal History/Biography: the Birth of the Internet." http://www.lk.cs.ucla.edu/personal_history.html (accessed January 9, 2012).